

Instructional Scenario

Cyber Defense



Course/Duty Area: Cybersecurity Fundamentals/Understanding Cyber Threats and Vulnerabilities

Scenario:

You are newly hired as a cybersecurity analyst for an organization that has recently experienced multiple cybersecurity incidents, including phishing campaigns targeting employees, malware infections on workstations, and concerns about unpatched systems exposing critical business data. Executive leadership has tasked your team with identifying cyber threats, understanding vulnerabilities, and recommending practical protections to reduce organizational risk while maintaining business operations and productivity.

Big Question:

How do cyber threats exploit vulnerabilities, and what can organizations do to reduce risk while maintaining usability and access?

Focused Questions:

- What is the difference between a cyber threat and a vulnerability?
- How do common cyber threats such as phishing, malware, and denial-of-service attacks work?
- Who are the different types of threat actors, and what motivates them?
- What characteristics make systems vulnerable to attack?
- How can organizations prevent, detect, and protect against cyber threats?
- How do organizational technology practices increase or reduce cybersecurity risk?

Student Project or Outcome:

Students will work in teams to complete a Cyber Threat and Vulnerability Risk Brief. Each team will

- identify assets, threats, and vulnerabilities affecting the organization
- analyze common cyber threats and threat actors
- explain how vulnerabilities are exploited
- recommend layered security controls and user training strategies
- evaluate organizational practices that may introduce additional cyber risk and propose mitigation strategies.

Teams will present their findings as a short briefing to the organization's leadership (i.e., teacher and other students).

Project-Based Assessment:

Cyber Threat and Vulnerability Risk Brief (Primary Assessment)

Students act as cybersecurity analysts preparing a professional risk brief for organizational leadership.

Project Deliverables

- Identification of at least three organizational assets
- Differentiation between threats and vulnerabilities affecting those assets
- Analysis of common cyber threats (e.g., phishing, malware, DoS/DDoS)
- Identification of likely threat actors and their motivations
- Description of vulnerabilities and how they could be exploited

- Recommended prevention and protection strategies using layered security controls
- Optional inclusion of emerging threats (AI-enabled phishing, supply-chain attacks)

Format Options: Written report, slide deck, or executive briefing document

Alternative Projects:

Threat Actor Profile and Attack Scenario

Students research and profile a specific type of threat actor and design a realistic attack scenario.

Project Deliverables

- Threat actor classification (e.g., cybercriminal, nation-state, insider, hacktivist)
- Motivation and typical targets
- Step-by-step explanation of a likely attack method
- Identification of vulnerabilities exploited
- Impact on confidentiality, integrity, and availability (CIA triad)
- Defensive controls that could prevent or detect the attack

Format Options: Infographic, one-page brief, or short presentation

Malware Analysis and Defense Plan

Students investigate a specific type of malware and create a defense strategy.

Project Deliverables

- Malware type overview (e.g., virus, worm, ransomware, botnet, spyware)
- Method of propagation
- Real-world example or case study
- Potential impact on an organization
- Detection and prevention techniques (e.g., antivirus, patching, user awareness)

Format Options: Digital poster, report, or narrated slide presentation

Vulnerability Case Study

Students analyze a real-world vulnerability using publicly available Common Vulnerabilities and Exposure (CVE) information.

Project Deliverables

- Overview of the selected CVE
- Description of the vulnerability and affected systems
- Explanation of how the vulnerability could be exploited
- Associated risks to systems or data
- Mitigation strategies and patches

Format Options: Case study worksheet, presentation, or analyst summary

Organizational Security Improvement Plan

Students evaluate an organization's security posture and propose improvements.

Project Deliverables

- Identification of common organizational security weaknesses

- Mapping of weaknesses to threats and vulnerabilities
- Recommended technical controls (e.g., firewalls, IDS/IPS, patch management)
- Recommended administrative controls (e.g., policies, training, procedures)
- Alignment to NIST Cybersecurity Framework functions

Format Options: Security plan document or briefing presentation

Teacher Resources:

- [Virginia Cyber Range](#)
- [NIST Cybersecurity Framework](#)
- [Common Vulnerabilities and Exposures \(CVE\) Database](#)
- [MITRE CVE](#)
- [Cybersecurity and Infrastructure Security Agency \(CISA\)](#)
- **Organizational Security Policy Examples (Industry & Government)**
Real-world policy examples students can analyze and reference.
 - [NIST Information Security Policies & Publications](#)
 - [CISA Security Policies & Best Practices](#)
 - [SANS Sample Security Policy Templates](#)
- **Sample Phishing Emails & Malware Case Studies**
Realistic examples for analysis, awareness training, and classroom labs.
 - [CISA Phishing Guidance and Examples](#)
 - [Google Phishing Quiz \(Student-Friendly Practice\)](#)
 - [SANS Security Awareness Case Studies](#)

Scenario submitted by Kristi Rice, Spotsylvania High School, Spotsylvania County Public Schools